

OFFICE OF THE DIRECTOR
DEPARTMENT OF MOTOR VEHICLES
Audits Office
P.O. BOX 932328 MS H-230
SACRAMENTO, CA 94232-3280



November 21, 2008

A- 40-9050

Patrick Duterte, Director
Solano County Health and Social Services Department
275 Beck Avenue, MS 5-200
Fairfield, CA 94533

Dear Mr. Duterte:

The California Department of Motor Vehicles' (DMV) Audits Office audit of the Solano County Health and Social Services Department (SCHSS) Government Requester Accounts is complete. The audit was based on the Memorandum of Understanding (MOU) between DMV and SCHSS, and applicable statutes and regulations stated in the California Vehicle Code and the California Code of Regulations. The fieldwork evaluation performed included observation at two SCHSS units; Special Investigations Unit and the Child Welfare Services (CWS) Unit.

We conducted the audit in accordance with *Government Auditing Standards* promulgated by the United States General Accountability Office. In general, the objectives were to determine if SCHSS:

- Internal controls are adequate to safeguard information obtained from DMV;
- Complies with the provisions of the MOU;
- Adheres to applicable rules and regulations governing the processing, storage, and transmission of DMV information.

Overall we found the current security controls in effect at SCHSS sufficient to meet the security objectives of this audit. However, during the audit we identified an item associated with the SCHSS CWS Unit that warranted corrective action.

The finding is detailed in the attached final report in the *Finding and Recommendation* section. Briefly stated, we found that Information Security Statements were not maintained for CWS employees. CWS Management implemented corrective action to resolve the finding during the audit. Therefore no written response is required to this report.

FINAL AUDIT REPORT

SOLANO COUNTY HEALTH AND SOCIAL SERVICES DEPARTMENT

JULY 1, 2007 THROUGH JUNE 30, 2008

#A - 40 - 9050

TABLE OF CONTENTS

COVER MEMO	i
EXECUTIVE SUMMARY.....	1
BACKGROUND	1-2
OBJECTIVES, SCOPE, AND METHODOLOGY	2
FINDINGS AND RECOMMENDATIONS.....	3-4
FINDING #1: Information Security Statements Not Maintained By CWS Employees	
CONCLUSION.....	4

EXECUTIVE SUMMARY

The California Department of Motor Vehicles (DMV) Information Services Branch (ISB) operates an information requester program that allows external entities to access DMV records pursuant to applicable statutes of the California Vehicle Code (CVC) and California Code of Regulations Title 13, Article 5 except as prohibited by CVC Section 1808.21. As an authorized DMV Government Requester Account holder the Solano County Health and Social Services Department (SCHSS), has access to basic record and address information on California Driver License, Vehicle Registration, Occupational License, Financial Responsibility, and Social Security. In accordance with its DMV Government Requester Memorandum of Understanding (MOU), SCHSS is allowed to make California DMV inquiries for its business needs.

The California Vehicle Code mandates that DMV protect the privacy rights of the public by releasing only certain information authorized by statutes. Statutes and regulations allow for businesses and individuals to access DMV records containing both confidential and non-confidential information, contingent upon approval of an application and compliance with the program requirements. DMV is dedicated in its mission of securing personal information for consumer protection. To meet our obligation of protecting the public and DMV information, we reviewed SCHSS compliance with the MOU, and applicable California laws and regulations.

We conducted the audit fieldwork at the SCHSS Central Office in Solano County, California September 23, 2008 and October 1, 2008. Our audit included an examination of SCHSS information technology operations, the DMV data security environment, evaluation of the network security architecture, the administrative security procedures, and of monitoring programs that are in place to protect DMV information.

Our evaluation found that SCHSS is approved for [REDACTED] requester codes, [REDACTED] codes. The [REDACTED] code is assigned to SCHSS Special Investigation's Unit and the [REDACTED] requester code is assigned to SCHSS Child Welfare Services (CWS) unit. The Special Investigation's Unit obtains requests directly through the Department of Justice using the California Law Enforcement Telecommunications Service (CLETS) system. The current security controls in effect at SCHSS as of October 1, 2008 are sufficient to meet the security objectives of this audit, except as noted in the *Finding and Recommendation* section of this report. However, because of inherent limitations in control systems, errors or irregularities may occur and not be detected. The finding is summarized as follows:

- Information Security Statements Not Maintained by CWS Employees

BACKGROUND

SCHSS was initially authorized as a Government Requester Account in 1987. SCHSS was assigned [REDACTED] requester codes, [REDACTED] with the following access to DMV information:

- Driver license – to help determine physical descriptions, addresses and age of subjects suspected of welfare fraud.
- Vehicle registration – to help verify vehicles owned, and to verify place of residence of those suspected of welfare fraud.
- Financial responsibility – to help determine how much money a suspect is spending per month to live.
- Occupational license – to help verify whether or not a suspected client is employed and where he/she may be working.

An addendum to the on-line requestor code granted SCHSS [REDACTED] access as of August 5, 2008. We found no inquiries made using the assigned [REDACTED] requester code during the twelve months period July 1, 2007 through June 1, 2008. However, the SCHSS CWS unit makes use of [REDACTED] requester code access to California Driver License information to locate absent parent. Requests are submitted by certified mail using the DMV form INF 254 directly to DMV Information Services Branch, Accounts Processing Unit (APU). Once the request is processed the information is returned certified to requester.

OBJECTIVES, SCOPE, AND METHODOLOGY

DMV is responsible for administering statewide programs that use and rely on information assets whether they are electronically stored or hard copy documents. A structure of laws, regulations, administrative requirements, and security requirements determine the permissive uses and necessary protection of this information.

DMV conducts audits and evaluations of entities accessing the information of the Department, to ensure that these entities abide by the applicable laws and regulations and other departmental requirements. The MOU, *California DMV Government On-Line Security Requirements*, and standards developed by the *National Institute of Standards and Technology*, are the primary criteria for this review.

The audit objectives were to verify compliance with the requirements of the MOU, as well as applicable statutes and regulations stated in the California Vehicle Code and the California Code of Regulations; and review the security procedures that SCHSS has in place to ensure the protection of DMV information. This included evaluation of SCHSS information systems security architecture, administrative procedures, and applicable monitoring programs.

FINDING AND RECOMMENDATION

FINDING – Information Security Statements Not Maintained By CWS Employees

Condition: During the audit, we interviewed the Manager of the SCHSS CWS unit. The Manager informed DMV Auditors that CWS did not have any Information Security Statements (INF 1128's) on file for employees that accessed DMV information. The Manager provided signed security statements during the fieldwork portion of the review and agreed to maintain on file going forward.

Criteria: The California Department of Motor Vehicles Government Requester Account Requirements, Security Requirements, paragraph number 3, items (a) and (b) states:

- a. *"Requester shall require every employee and the system administrator, having direct or incidental access to Department records, to sign a copy of the Information Security Statement (INF 1128). The INF 1128 is required upon initial authorization for access to Department records and annually thereafter. A copy of the Requester's signed statement(s) shall be maintained on file at Requester's worksite for at least two years following the deactivation or termination of the authorization and shall be available to Department upon demand.*
- b. *Requester shall restrict the use and knowledge of requester codes and operational manuals to employees who have signed an Information Security Statement (INF 1128)."*

In addition, the MOU #9 states, in part:

"Requester agrees to establish security procedures to protect the confidentiality of DMV records and access information, as required by California Vehicle Code Section 1808.47. Requester shall ensure that each Requester's employee having direct or incidental access to DMV records has signed an individual security statement. That statement shall contain, at a minimum, the same provisions contained within the DMV's Information Security Statement, form INF 1128. Requester shall ensure that each person working on behalf of Requester having direct or incidental access to DMV records has signed the Information Security Statement, form INF 1128. The form shall be maintained on file, and made available to DMV upon request."

Failure to maintain current copies of the INF 1128 on file weakens the internal controls for the security measure that have been established by DMV.

Recommendation: SCHSS should ensure each employee authorized with direct or incidental access to DMV records sign an INF 1128 upon initial authorization for access and annually thereafter. SCHSS should maintain a copy on file for at least two years following deactivation or termination of authorization.

CONCLUSION

SCHSS operates a system and program that permits its authorized end users access to DMV information, and provides assurance that access to the information is appropriately controlled and monitored in accordance with the requirements of its Memorandum of Understanding. Accordingly, the mechanisms and controls in place to protect information received from DMV taken as a whole are sufficient and functioning properly to fulfill the program objectives. The audit resulted in a finding related to security requirements; the SCHSS did not maintain Information Security Statements for employees with authorized access to DMV records.

SCHSS concurs with the finding and provided acceptable corrective action.

GRACE M. RULE-ALI, MANAGER,
Information Systems-Requester Audit Section
Audits Office
(916) 657-5828

November 18, 2008

Review Team:

Benedicta Ikhala, Auditor In Charge
Andrew Lau, Auditor
Anthony Allen, Auditor